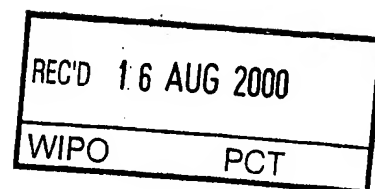


BEST AVAILABLE COPY



DE00/01796

EJU

**Prioritätsbescheinigung über die Einreichung
einer Patentanmeldung**

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Aktenzeichen: 199 25 693.4

Anmeldetag: 4. Juni 1999

Anmelder/Inhaber: Dr. Peter Wratil, Rosengarten Kr Harburg/DE;
Phoenix Contact GmbH & Co, Blomberg, Lippe/DE.

Bezeichnung: Schaltungsanordnung zur gesicherten Datenübertra-
gung in ringförmigen Bussystemen

IPC: H 04 L, G 05 B

BEST AVAILABLE COPY


Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ur-
sprünglichen Unterlagen dieser Patentanmeldung.

München, den 8. August 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Seller

Patentanmeldung

Datum: 3.6.1999 (Dr. Peter Wratil)

 Darf nicht geändert werden

Anmelder:

1. Dr. Peter Wratil
Heinrich-Wildung-Weg 3
21224 Rosengarten-Klecken
Tel.: 04105-7363
2. Phoenix Contact GmbH & Co.
Postfach 1341
D-32819 Blomberg

Herren: Karsten Meyer-Gräfe, Thorsten Behr, Wolfram Kreß

Schaltungsanordnung zur gesicherten Datenübertragung in ringförmigen Bussystemen

Zusammenfassung

Die vorliegende Schaltungsanordnung erlaubt es, an ringförmigen Standardbussystemen Daten zu übertragen, die für den Aufbau fehlertoleranter Strukturen notwendig sind. Zur Realisierung benötigt man eine Überwachungseinheit und dezentrale Ein- und Ausgabeeinheiten, die Daten zur Regelung oder Steuerung senden oder entgegennehmen. Die Schaltungsanordnung übernimmt die Aufgabe, eventuelle Fehler zu erkennen, die für den Prozeß innerhalb einer Maschine oder Anlage zur Gefahr werden können. Durch den internen Aufbau identifiziert die Schaltungsanordnung bereits vor der Fehleroffenbarung zum Prozeß einen eventuellen Fehler und leitet eine gesicherte Abschaltung ein. Dabei ist es gleichgültig, ob die externe Steuerung oder das verwendete Bussystem für den Fehler verantwortlich ist.

Beschreibung des Verfahrens und Darstellung des Standes der Technik

Im Maschinen- und Anlagenbau werden heute nicht selten Bewegungen und Vorgänge gesteuert oder geregelt, die im Fehlerfall oder bei Versagen eine Gefahr für das Leben und die Gesundheit von Personen darstellen. Neben diesen Gefahren gilt es aber auch wertvolle Maschinenteile zu schützen, die bei möglichen Fehlfunktionen hohe finanzielle Schäden verursachen können.

Eventuell auftretende Fehler müssen daher durch den Prozeß erkannt werden, und die Maschine sollte in einen Zustand geführt werden, der als gefahrlos anzusehen ist. In der Regel sind hierfür redundante Strukturen notwendig, die unabhängig von der eigentlichen Steuerung oder Regelung die Sicherheitsfunktionen überwachen. Im Maschinen- oder Anlagenbau ist zur Fehlererkennung in der Regel eine Feststellung eines Einfach-Fehlers hinreichend. Nach Erkennen dieses Fehlers kann dann der Prozeß abgebrochen werden und in einem sicheren Zustand verweilen. Ein eventueller Schaden durch die fehlerhafte Fortführung des Prozesses ist damit unterbunden.

Die Verfahren zur Fehlererkennung und deren notwendige Maßnahmen sind in den internationalen Normen (DIN V VDE 0801 und DIN ISO 61508) festgehalten. Durch die Grundlagen dieser Normen haben die Hersteller von Automatisierungseinrichtungen in den letzten Jahren unterschiedliche Strategien entwickelt, die sichere Übertragungen an Bussystemen erlauben (Profibus mit F-Profil, PNO und Safety-Bus P, Fa. Pilz und Sick). Zusätzlich wird es in Kürze Steuerungen auf dem Markt geben, die bereits intern redundante Strukturen aufweisen und so im Zusammenspiel mit den genannten sicheren Bussystemen eine Fehlererkennung zulassen (z.B.: Fa. Siemens S 7 400 F oder Pilz PSS 3000-Serie). Diese Verfahren lassen sich jedoch nur bei vollständig neuer Installation der notwendigen Komponenten einsetzen und schützen nur mangelhaft gegen systematische Fehler. Die hier vorgestellte Schaltungsanordnung macht es sich viel mehr zur Aufgabe, Fehler in einem Prozeß zu erkennen, der lediglich mit Standardeinheiten aufgebaut ist. Darüber hinaus werden nicht nur eventuelle Fehler beim Datentransport über ein verwendetes Bussystem, sondern auch Störungen oder Programmierfehler in der Steuerungseinrichtung erkannt und eliminiert. Die Schaltungsanordnung stellt damit eine Realisierung eines Verfahrens vor, das bereits unter dem Patent Nr. 198 57 683.8 angemeldet wurde. Das Verfahren eignet sich für alle ringförmigen Bussysteme, wobei die beschriebene Technik optimal auf den Interbus (Phoenix Contact) abgestimmt ist. Hier wurde bereits Anfang 1999 ein Anforderungsprofil erarbeitet und veröffentlicht (Zeitschrift IEE, April 1999, Karsten Meyer-Gräfe: Interbus goes Safety).

Die Fig. 1 zeigt den notwendigen Aufbau für ein derartiges System. Die Steuerung (1) übernimmt im Prozeß alle Steuerungs- und Regelfunktionen. Sie erkennt auch mögliche Fehler und kann Prozesse unterbrechen oder in einen sicheren Zustand führen. Im Falle eines eigenen Versagens oder bei fehlerhaftem Datentransport ist sie jedoch nicht in der Lage, den gewünschten sicheren Zustand herbeizuführen. Dieser Ausfall ist auch dann gegeben, wenn in dem Steuerungssystem bereits eine weitgehende Trennung von Prozeßsteuerung und Sicherheitskontrolle vorliegt. Da es auch hier keine Redundanz gibt, wird ein unerkannter Fehler möglicherweise schwerwiegende Folgen haben. Entsprechend der Erfindung werden weitere Komponenten hinzugefügt, die einen möglichen Fehler erkennen und eliminieren. Diese Einheiten sind: Eine Überwachungseinheit (4) und eine oder mehrere dezentrale Einheiten im Prozeß (9), die nur dort notwendig sind, wo Daten mit Sicherheitsbezug empfangen oder gesendet werden.

Die Steuerung (1) beinhaltet ein Daten-Abbild-Register (2), das alle Ausgangsdaten und weitere Kontrollsignale über die Datenleitung (13) zu den peripheren Einheiten (4,7,8,9,12) sendet. Da der Bustransport ähnlich wie ein Schieberegister funktioniert, senden alle peripheren Einheiten über die Rückleitung (14) im gleichen Buszyklus ihre Eingangsdaten zur Steuerung, die im Daten-Abbild-Register (3) zur Verfügung stehen. In einem folgenden SPS-

Zyklus verarbeitet die SPS nun die Daten aus ihren beiden Abbild-Registern und erzeugt so den notwendigen Zustand für den Prozeß. Ohne die Einheiten (4) und (9) ist sie jedoch nicht in der Lage, einen Programmierfehler, einen Zustand durch Störung oder Ausfall oder einen Datenfehler durch falschen Bustransport zu regeln. Die Überwachungseinheit (4) beinhaltet daher einen eigenen Mikroprozessor, der die gesendeten Daten der SPS überwacht und nur die sicherheitsrelevante Größen auf Sinnfälligkeit untersucht. So ist die Überwachungseinheit (4) mit der Transfer-Einheit (5) in der Lage, die SPS zu überwachen. Sie kann aber noch zusätzlich über die im Rücklauf installierte Transfer-Einheit (6) auch die Daten der Eingänge der dezentralen Einheiten lesen. Da die sicherheitsrelevante Einheit (9) ihre Ausgangsinformation (D3) auch direkt an die Eingangseinheit (C3) weitergibt, gelingt so eine direkte Kontrolle, ob der Bustransfer ordnungsgemäß funktioniert hat.

Ferner ist die Überwachungseinheit mit ihrer Transfer-Einheit (5) auch in der Lage, die Daten für die sicherheitsrelevante dezentrale Einheit (9) zu manipulieren. Sie kann insbesondere Daten der SPS überschreiben und so eine Zustimmung zur Datenausgabe von (9) unterbinden. Die dezentrale Einheit wird nur dann aktiv, wenn sie über die Kontroll-Einheit (11) eine Zustimmung für die Daten der Ausgabe-Einheit (10) erhalten hat.

Das Timing mit dem Datentransport ist in der folgenden Tabelle gezeigt:

Sh	MT	ST		1		2		D3		C3		4		SR		MR
		A	E	A	E	A	E	A	E	A	E	A	E	A	E	
0	LBW		ST		E1		E2		E3		EC3		E4		ESR	
1	ASR	LBW	LBW	ST	ST	E1	E1	E2	E2	E3	E3	EC3	EC3	E4	E4	ESR
2	A4	ASR	ASR	LBW	LBW	ST	ST	E1	E1	E2	E2	E3	E3	EC3	EC3	E4
3	1	A4	A4	ASR	ASR	LBW	LBW	ST	ST	E1	E1	E2	E2	E3	E3	EC3
4	A3	1	AC3	A4	A4	ASR	ASR	LBW	LBW	ST	ST	E1	E1	E2	E2	E3
5	A2	A3	A3	AC3	AC3	A4	A4	ASR	ASR	LBW	LBW	ST	ST	E1	E1	E2
6	A1	A2	A2	A3	A3	AC3	AC3	A4	A4	ASR	ASR	LBW	LBW	ST	ST	E1
7	ST	A1	A1	A2	A2	A3	A3	AC3	AC3	A4	A4	ASR	ASR	LBW	LBW	ST
8		ST	ST	A1	A1	A2	A2	A3	A3	AC3	AC3	A4	A4	ASR	ASR	LBW

Das Timing-Diagramm zeigt den Zustand nach jeder Schiebe-Information im Ring (Beispiel: Interbus). Die Information AC3 ist von der Überwachungseinheit (4) mit der Transfer-Einheit (5) manipulierbar und kann überschrieben werden. Somit erhält die dezentrale Einheit (9) in ihrer Kontroll-Logik (11) eine Zusatz-Information, die eine fehlerhafte Ausgabe unterbindet. Wie aus dem Timing-Diagramm ebenfalls ersichtlich ist, kann die Überwachungseinheit (9) auch die Daten der Ausgabe von (9) lesen (EC3). Diese Daten stellen die direkte Ausgabe-Information der Einheit (9) dar, so daß ein Busfehler sicher erkannt wird.

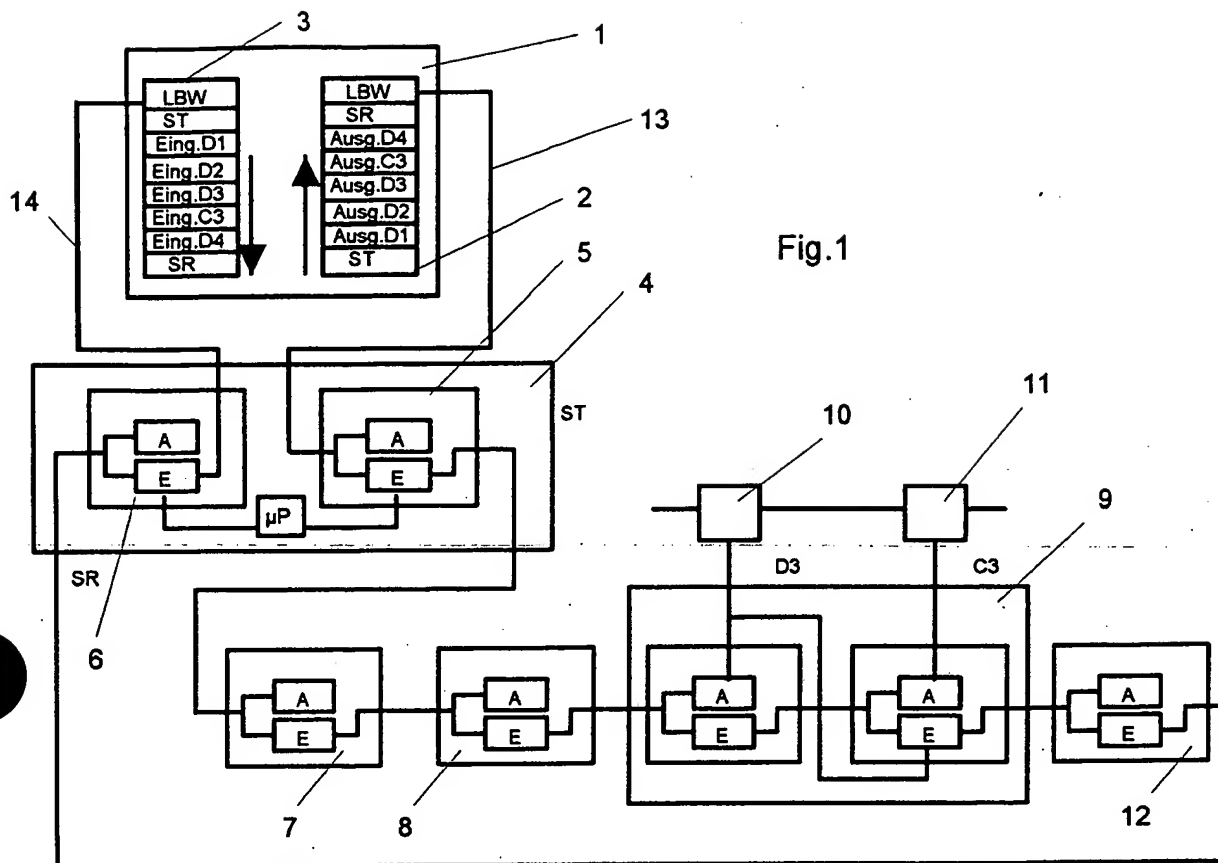
Der interne Aufbau der sicherheitsrelevanten dezentralen Einheit (9) ist in Fig. 2 dargestellt. Sie (1) besteht aus zwei Busbausteinen (2,3), so daß Eingangsinformationen redundant vom Prozeß geholt werden können (4,5). Zusätzlich wird die Ausgabeinformation (Dn) von (2) über den Eingangsteil der anderen Einheit (3) abgebildet. Ein möglicher Fehler bei der internen Ablage oder beim Bustransport wird damit im Folge-Zyklus des Bustransports erkannt. Die Ausgabeinformation von Dn wird von der Steuerung (SPS) in den Zwischenspeicher (7) geschrieben. Die Kontroll-Logik (6) entscheidet aber zusätzlich darüber, ob die Information des Zwischenspeichers (7) über die Ausgabe-Logik (8) an der Peripherie erscheint. Sie (6) kann entweder die gespeicherte Information freigeben (über die Leitung 10) oder den Zustand löschen (über die Leitung 11), so daß der Ausgang (9) den Prozeß in einen sicheren Zustand bringt.

Die Schaltungsanordnung funktioniert daher im Prinzip genauso, wie ein normales dezentrales SPS-System. Die Komponenten erlauben es lediglich zusätzlich, Eingänge redundant zu überwachen und gespeicherte Ausgabeinformationen vor der Ausgabe auf Sinnfälligkeit zu untersuchen. Ferner kann die Überwachungseinheit auch Fehler erkennen,

die nicht nur durch Ausfall oder Störung zustande gekommen sind, sondern einen Programmier- oder Parametrierfehler als Ursache hatten.

Patentansprüche

1. Schaltungsanordnung zur gesicherten Datenübertragung in ringförmigen Bussystemen, **dadurch gekennzeichnet**, daß eine Überwachungseinheit (Fig. 1,4) die von der Steuerung (1) ausgesendeten Daten über eine Transfer-Einheit (5) kontrolliert und auf mögliche Fehler untersucht und im Fehlerfall die Freigabe-Daten für eine sicherheitsrelevante dezentrale Einheit (9) unterdrückt oder löscht, so daß ein möglicher Fehler nicht in den Prozeß gelangen kann, und zusätzlich die bereits zwischengespeicherten Daten der peripheren Einheit (9) über eine zweite Bus-Einheit rückliest und derart mögliche Transportfehler durch die Kontroll-Logik (6) überwacht und einen sicheren Zustand der Ausgabe (10) für den Prozeß einleitet, **dadurch gekennzeichnet**, daß die sicherheitsrelevante periphere Einheit (9) nicht nur die zwischengespeicherte Ausgabe (D3) sondern auch eine redundante Eingabe für die Überwachungseinheit (4) zur Verfügung stellt.
2. Schaltungsanordnung nach dem Anspruch 1, **dadurch gekennzeichnet**, daß im Prozeß sicherheitsrelevante dezentrale Einheiten eingebracht werden können (Fig.2), die über redundante Eingabe-Kanäle (4,5) verfügen und so den angeschlossenen Prozeß redundant überwachen und einen Fehler erkennen.
3. Schaltungsanordnung nach den Ansprüchen 1 bis 2, **dadurch gekennzeichnet**, daß die sicherheitsrelevanten Einheiten (Fig.2) über einen Zwischenspeicher (7) verfügen, der von einer zweiten Bus-Einheit (3) rückgelesen wird und so noch vor der Freigabe zum Prozeß (über die Ausgabe (8) mit den Signalen (9) von der Überwachungseinheit (Fig.1, 4) kontrolliert wird.
4. Schaltungsanordnung nach den Ansprüchen 1 bis 3, **dadurch gekennzeichnet**, daß die angesprochenen peripheren Einheiten auch selbst logische Verknüpfungen durchführen können und so im Gesamtverbund eine höhere Prozeßgeschwindigkeit erreicht wird.
5. Schaltungsanordnung nach den Ansprüchen 1 bis 4, **dadurch gekennzeichnet**, daß die Überwachungseinheit auch selbst Steuerungsfunktionen übernehmen kann und so ein Verbund mit einer Sicherheitssteuerung entsteht.
6. Schaltungsanordnung nach den Ansprüchen 1 bis 5, **dadurch gekennzeichnet**, daß die sicherheitsrelevante dezentrale Einheit mit nicht sicherheitsrelevanten Standard-Bausteinen zum Busverkehr auskommt und keinerlei sicherheitsrelevante Spezialbausteine benötigt und somit preisgünstig und technologisch abgesichert funktioniert.
7. Schaltungsanordnung nach den Ansprüchen 1 bis 6, **dadurch gekennzeichnet**, daß die Funktion bei Standard-Bussystemen betriebsfähig ist und somit ohne zusätzliche Installation von weiteren Bussystemen oder speziellen Komponenten auskommt.
8. Schaltungsanordnung nach den Ansprüchen 1 bis 7, **dadurch gekennzeichnet**, daß die Funktion durch Hinzufügen der Überwachungseinheit (Fig. 1,4) und durch Austausch von normalen dezentralen Einheiten durch sicherheitsrelevante Einheiten (Fig.1, 9) nachträglich installierbar ist.
9. Schaltungsanordnung nach den Ansprüchen 1 bis 8, **dadurch gekennzeichnet**, daß die Sicherheitsfunktion des Systems auch nachträglich durch Hinzufügen von Hardware-Elementen oder Software-Bausteinen erweiterbar ist.



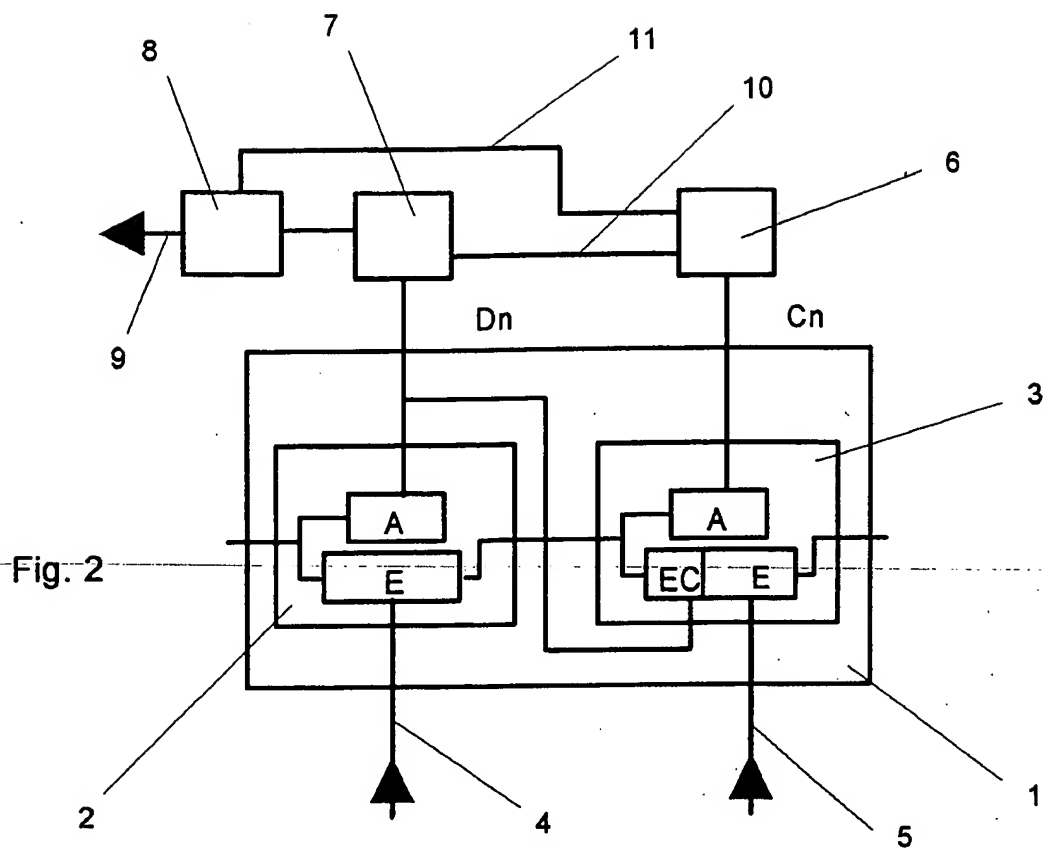


Fig. 2